BLACK BELT SECURE
Defend Today, Thrive Tomorrow.

Legacy Exchange Servers Remediation Checklist
Microsoft Exchange (2013 & 2016)

Note:

Exchange Server 2013 (end of support: April 11, 2023) and **Exchange Server 2016 (end of support: October 14, 2025)** are both fully unsupported. No security updates, bug fixes, time zone adjustments, or Microsoft technical support are available. Running these exposes your organization to severe risks: unpatched vulnerabilities (prime targets for exploits like ransomware or data breaches), potential mail flow disruptions (especially in any hybrid scenarios via Microsoft's Transport Enforcement for persistently vulnerable servers), compliance failures, and interoperability issues with modern clients or Exchange Online.

1. **Immediate Risk Assessment & Inventory**
    - Inventory all Exchange 2013/2016 servers (roles: Mailbox, Client Access, Edge Transport; versions/CUs; hybrid config status).
    - Identify remaining on-premises mailboxes, public folders, resources, connectors, or apps relying on these servers.
    - Check for hybrid dependencies (e.g., Azure AD Connect/Entra ID sync, free/busy, mail flow).
    - Run health checks (e.g., Microsoft Exchange Health Checker script) and review logs/IIS for signs of compromise.
    - Document risks: No patches since EOS dates → heightened exploit exposure; potential blocking/throttling from Exchange Online; compliance/regulatory exposure (e.g., GDPR, HIPAA if applicable).

2. **Prioritize Migration Paths (Target: Exchange Online for Most)**

    - For migrated users (already in Microsoft 365): Confirm full cutover (MX/Autodiscover pointed to Exchange Online; no on-premises dependencies). Proceed directly to decommissioning (Step 4).
    - For remaining on-premises users: Migrate mailboxes/public folders/resources to Exchange Online (use hybrid migration if coexistence needed temporarily; otherwise cutover/staged/IMAP). Leverage Microsoft FastTrack or partners.
    - Alternative (if on-premises required): Upgrade to Exchange Server Subscription Edition (SE) — but note: No direct in-place from 2013; 2016 requires legacy upgrade path first (complex/time-consuming). Coexistence with unsupported versions blocked in newer SE CUs.
    - Temporary option: If migration delayed, explore paid Extended Security Updates (ESU) for 2016/2019—but limited duration/availability post-2025 EOS, not for 2013.

3. **Preparation & Prerequisites**

    - Update to latest supported CUs (if still accessible via ESU for 2016).
    - Test backups, disaster recovery, and rollback.
    - Address dependencies: Certificates, authentication (modern auth preferred), Windows Server versions.
    - Use Microsoft's Exchange Deployment Assistant (setup.cloud.microsoft/exchange) for migration guidance.
    - If hybrid: Validate connectors, OAuth, directory sync; migrate public folders if needed.

4. **Execute Migration & Decommission (Critical for Already-Migrated Users)**
    - Migrate any straggling mailboxes/resources to Exchange Online.
    - Reconfigure mail flow, Autodiscover, etc., to point fully to cloud.
    - For decommissioned servers (post-migration):
        - Verify no connections (logs for OWA, ActiveSync, EWS, etc.).
        - Place in maintenance mode → soft-shutdown → monitor.
        - Uninstall Exchange via setup (preferred over forced removal).
        - Clean Active Directory: Remove server objects, connectors, SCPs, certificates, DNS records.
        - If no directory sync needed: Disable Azure AD Connect/Entra sync → fully remove Exchange/hybrid config.
        - If sync retained: Keep minimal Exchange management tools (e.g., 2019 CU12+) for attribute management; otherwise, use PowerShell/ADUC alternatives.
    - Test thoroughly: Client connectivity, mail routing, compliance.

5. **Post-Remediation & Ongoing**
    - Update inventories, documentation, DR plans.
    - Communicate completion to executives/stakeholders.
    - Monitor Exchange Online for stability/patches.
    - Schedule audits to prevent future legacy accumulation.

Security Recommendations (Check for Compromise)

6. **Check for Evidence of Compromise (Pre-Remediation Security Sweep)**
   Unsupported Exchange 2013/2016 servers are high-risk for historical and ongoing exploitation (e.g., webshells from ProxyLogon/ProxyShell-style attacks, credential theft, backdoors). Perform these checks immediately on all servers—assume compromise until proven otherwise. Document findings thoroughly.

   - **Run Microsoft's Exchange Server Health Checker Script (Primary starting point)**
     Download the latest version from: https://github.com/microsoft/CSS-Exchange/releases/latest/download/HealthChecker.ps1
     Run as Administrator in Exchange Management Shell: .\HealthChecker.ps1 (or specify servers: .\HealthChecker.ps1 -Server EXCH01,EXCH02)
     - Review output/HTML report for: security vulnerabilities, missing patches (will flag many due to EOS), unusual configurations, or warnings that could indicate tampering.
     - This script evolves and includes checks for known issues; it won't detect all malware but highlights red flags.
   - **Scan for Known Indicators of Compromise (IOCs)**
     - Focus on common post-exploitation artifacts from legacy Exchange attacks:
       - Webshells in IIS/Exchange directories (e.g., OWA, ECP, Autodiscover virtual dirs): Look for suspicious .aspx, .asp, .php files like ChinaChopper variants (e.g., names like errorEE.aspx, log.aspx, or random strings). Check paths:
         C:\inetpub\wwwroot\owa\auth\
         C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\ (and similar for ECP/ECP)
       - Suspicious files: Search for .aspx/.asp files with recent modification dates or unusual content (e.g., base64-encoded PowerShell).

        - IIS logs: Review C:\inetpub\logs\LogFiles\W3SVC1\ (or other sites) for anomalous requests (e.g., non-standard User-Agents, POSTs to /owa/auth/, unusual IPs from known bad ranges, or exploit patterns like /ecp/default.aspx with suspicious parameters).
        - Event logs: Check Windows Security/Application logs for failed/successful logons from odd accounts, process creation (cmd.exe/PowerShell from IIS worker processes w3wp.exe), or events around known vuln exploitation periods.
        - Running processes/connections: Use Task Manager, Process Explorer, or netstat -ano / Get-NetTCPConnection for unexpected connections or child processes from Exchange services.
- **Additional Tools & Checks**
    - Microsoft's older but relevant scripts (from GitHub CSS-Exchange/Security repo):
        - Test-ProxyLogon.ps1 or similar legacy IOC scanners (adapt if needed; focus on log parsing for exploit patterns).
    - Endpoint detection tools: If available (e.g., Defender for Endpoint, third-party EDR), run full scans or hunt queries for webshells, credential dumping (e.g., Mimikatz indicators), or persistence (scheduled tasks, registry Run keys).
    - Network monitoring: Review firewall/IDS/egress logs for outbound connections from Exchange servers to unknown C2 IPs/domains (common post-compromise behavior).
    - If hybrid: Check Azure AD/Entra sign-in logs for anomalous access tied to on-premises accounts.
- **If Suspicious Activity/Compromise Found**
    - Do not proceed with normal decommissioning—risk spreading persistence/malware.
    - Isolate servers immediately (remove from network, block inbound/outbound).
    - Engage incident response/forensics team (internal or external).

    - Assume credential compromise: Rotate all service accounts, admin creds, and review for lateral movement.
    - Consider forensic imaging before any changes.
    - Report per compliance requirements (e.g., data breach laws).
- **Key Caveat**
  These steps provide reasonable indicators but are not definitive on unsupported systems. True security requires full migration to Exchange Online (or supported on-prem like Subscription Edition). Prioritize accelerating migrations for any remaining users.

Team Background & Expertise

Our remediation efforts are supported by Black Belt Secure, a national award-winning Managed Security Services Provider (MSSP).

With years of hands-on experience in cybersecurity, networking engineering, disaster recovery, and infrastructure projects, the team specializes in protecting businesses from evolving threats while enabling secure modernization.

Key strengths relevant to this Exchange 2013/2016 project include:

- **Incident Response & Compromise Assessment** — 24/7 SOC monitoring with rapid engagement (average 3.5 minutes on alerts), remote containment, remediation for threats like ransomware/phishing/endpoint breaches, and forensic-level checks for indicators of compromise (e.g., webshells, anomalous activity).
- **Legacy & Hybrid Infrastructure Expertise** — Building/maintaining secure on-premises environments (including Active Directory, DNS, servers, and domain backups) while supporting seamless transitions to cloud platforms like Microsoft 365/Exchange Online.
- **Migration & Modernization Support** — Technical consulting for on-prem-to-cloud projects, hybrid setups, risk assessments, vulnerability closure, and compliance roadmaps—ideal for decommissioning unsupported servers and migrating remaining mailboxes without spreading potential persistence.
- **vCISO Leadership via Jutsu Program** — Fractional CISO services (risk assessments, strategic reviews, board-ready reporting) under the proprietary Jutsu framework—an operational security model inspired by martial arts progression. It

transforms organizations from reactive "novice" to "Black Belt" mastery through structured stages: threat detection/prevention, compliance/risk management, incident response/recovery, employee training, and zero-trust implementation.

- **Broader Capabilities** — Auditing (network/security/cloud), disaster recovery (off-site backups/restore), BEC/email security, AI-driven threat intelligence, and tailored solutions for industries facing similar legacy risks.

The team's battle-tested professionals—cybersecurity virtuosos, technology visionaries, and relentless problem solvers—prioritize proactive defense ("Defend Today, Thrive Tomorrow") to minimize business disruption. This expertise ensures thorough compromise sweeps, safe migrations, and clean decommissions while aligning security with executive priorities.

For more details:

Peter Vavorksy,
blackbeltsecure.com (Contact: 469-557-2007 | pvavrosky@blackbeltsecure.com).

BLACK BELT SECURE
Defend Today, Thrive Tomorrow.